PRUEBA DE HABILIDADES PRACTICAS CCNA
EVALUACIÓN

CEFERINA MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA ELECTRÓNICA
CARTAGENA, 2020

PRUEBA DE HABILIDADES PRACTICAS CCNA
EVALUACIÓN

CEFERINA MARTINEZ

INFORME FINAL PARA LA OBTENCION DEL TITULO DE INGENIERIA DE SISTEMAS

HÉCTOR JULIÁN PARRA
ASESOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA INGENIERÍA ELECTRÓNICA
CARTAGENA, 2020

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Cartagena, Junio 10 de 2020

DEDICATORIA

Este logro va dedicado especialmente a las personas que son las principales patrocinadoras de este logro como lo son mis padres, por su amor, su trabajo y su sacrificio en todos estos años, gracias convertirme en lo que hoy soy. Es un orgullo y un privilegio ser su hijo, son los mejores padres que Dios pudo elegir para mí.

A mis hermanos (as) por estar siempre presentes, acompañándome y por el apoyo incondicional, que me brindaron a lo largo de esta etapa de mi vida.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos.

AGRADECIMIENTOS

Hoy en día y a través de todas las circunstancias que hemos tenido que pasar para estar donde estamos es indudable que debemos estar agradecidos primero con Dios por permitir que cada una de las actividades nos haya impactado en nuestro aprendizaje diario, pero también debemos dar gracias a cada una de las personas que nos han guiado en el transcurso de este diplomado ya que sin ustedes no podríamos haber asimilado y reforzado cada conocimiento que se trabajó a lo largo del mismo.

Contenido

Lista de tablas.

Lista de figuras

GLOSARIO.

Gns3: simulador grafico de red. Es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Con GNS3 los usuarios tendrán la posibilidad de poder escoger cada uno de los elementos que llegarán a formar parte de una red informática

Host: ordenador que funciona como punto de inicio y final de la transferencia de datos.

Networking: establecimiento de conexiones de interacción y trabajo. En el mundo de las computadoras, el concepto de networking aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos Una red o red de datos es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos

Protocolos de red: conjunto de reglas que rigen el intercambio de informacion. Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores.

Vlan: (Virtual local área), Red de área local que agrupa un conjunto de equipos de manera lógica y no física

RESUMEN.

La principal característica de un protocolo de enrutamientos es que esta permite compartir información entre los diversos ROUTERS de manera remota y actualizar de manera dinámica la información de enrutamiento a sus propias tablas y compartirlas entre sí.
La ventaja más significativa de los routers con protocolo dinámico es que este permite hacer un informe en el cambio de la topología (RUTAS) entre los distintos routers de la red y estos a su vez aprenden automáticamente las nuevas redes, así como las bajas de las mismas.

Podemos decir que uno de los primeros protocolos utilizados formalmente es el RIP en su versión, aunque muchos de los algoritmos usados en el son productos directos del abuelo ARPANET. Aun cuando el RIP ha evolucionado a su versión 2, este aun presenta algunos problemas de escalamiento, dejándolo atrás cuando se requiere de redes grandes, una mejor opción es usar versiones de protocolos más avanzados tales como el IGRP y el EIGRP, ambos productos de CISCO

PALABRAS CLAVE. CCNP, CISCO**,** Enrutamiento, Conmutación, Seguridad, Red.

ABSTRACT

We can say that one of the first protocols used formally is the RIP in its version, although many of the algorithms used in it are direct products of the grandfather ARPANET. Even though the RIP has evolved to version 2, it still presents some scaling problems, leaving it behind when large networks are required, a better option is to use more advanced protocol versions such as IGRP and EIGRP, both CISCO products.

The main characteristic of a routing protocol is that it allows to share information between the different ROUTERS remotely and dynamically update the routing information to its own tables and share them with each other.
The most significant advantage of routers with dynamic protocol is that it allows reporting in the change of the topology (ROUTES) between the different routers in the network and these in turn automatically learn the new networks, as well as the lows of the same.

1.1. KEYWORDS. CCNP, CISCO, Routing, Switching, Security, Network

3. INTRODUCCIÓN

Las redes modernas continúan evolucionando para adaptarse a la manera cambiante en que las organizaciones realizan sus actividades diarias. Ahora los usuarios esperan tener acceso instantáneo a los recursos de una compañía, en cualquier momento y en cualquier lugar. Estos recursos incluyen no solo datos tradicionales, sino también de video y de voz. También hay una necesidad creciente de tecnologías de colaboración que permitan el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación física.

Los distintos dispositivos deben trabajar en conjunto sin inconvenientes para proporcionar una conexión rápida, segura y confiable entre los hosts. Los switches LAN proporcionan el punto de conexión a la red empresarial para los usuarios finales y también son los principales responsables del control de la información dentro del entorno LAN. Los routers facilitan la transmisión de información entre redes LAN y, en general, desconocen a los hosts individuales. Todos los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching sobre la que se puedan basar. Esta infraestructura se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable necesaria.

4. OBJETIVOS.

4.1 Objetivo General.

Implementar una solución ante una problemática determinada en una pequeña empresa que quiere establecer un diseño de red que beneficie la conectividad y la eficiencia en el transporte de voz, audio y video en todas sus sucursales.

4.2 Objetivos Específicos:

1. configuración básica del Router, switches y dispositivos host
2. establecer protocolos de enrutamiento dinámico, ospf, nat y dhcp
3. solucionar posibles fallas en la conectividad.

5.DESARROLLO ESCENARIO 1

5.1 Escenario 1.

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

5.2 Topología

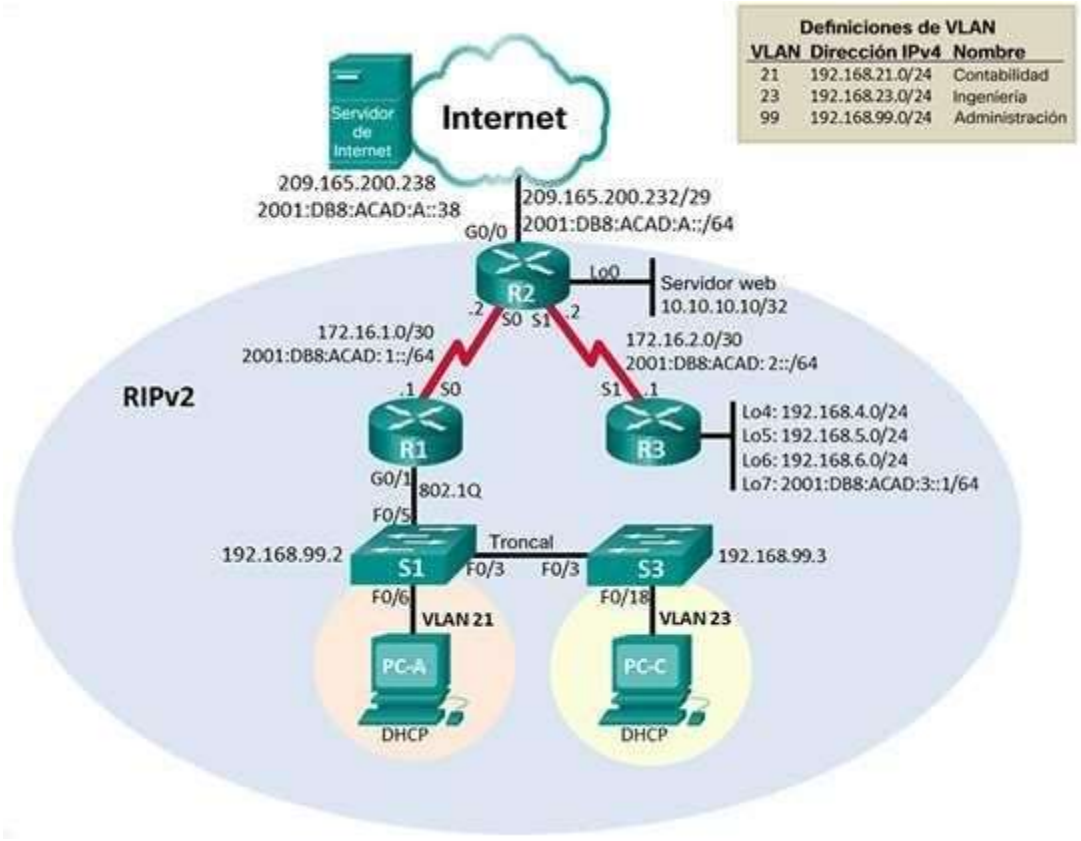


Figura 1 Tipología de escenario 1

5.3 Parte 1 Inicializar dispositivos.

5.3.1 Paso 1 Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1 Comando IOS

Tarea	***Comando de IOS***
Eliminar el archivo startup-config de todos los routers	*Router>enable* *Router#erase startup* *Router#erase startup-config* *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]* *Erase of nvram: complete* *%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram* *Router#*
Volver a cargar todos los routers	*Router#reload* *Proceed with reload? [confirm]ySystem Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)* *Technical Support: http://www.cisco.com* *Would you like to enter the initial configuration dialog? [yes/no]:n* *Press RETURN to get started!* *Router>*
Eliminar el archivo startup-config de todos los switches	*Switch>ena* *Switch#erase startup-config* *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]* *Erase of nvram: complete* *%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram* *Switch#*
y eliminar la base de datos de	*Switch#delete vlan.dat* *Delete filename [vlan.dat]?y*

VLAN anterior	*Delete flash:/y? [confirm]y%Error deleting flash:/y (No such file or directory)* *Switch#*
Volver a cargar ambos switches	*Switch#reload* *Proceed with reload? [confirm]yC2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)*
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	*Switch#show flash:* *Directory of flash:/* *1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin* *64016384 bytes total (59601463 bytes free)* *Switch#*

5.4 Parte 2. Configurar los parámetros básicos de los dispositivos

5.4.1 Paso 1. Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 2 Elemento o tarea de configuración

Elemento o tarea de configuración	***Especificación***
Dirección IPv4	*209.165.200.238*
Máscara de subred para IPv4	*255.255.255.248*
Gateway predeterminado	*209.165.200.233*
Dirección IPv6/subred	*2001:DB8:ACAD:A::38/64*
Gateway predeterminado IPv6	*2001:DB8:ACAD:A::32*

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

5.4.2 Paso 2 Configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 configuración para R1

Elemento o tarea de configuración	***Especificación***
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	***R1*** *Router(config)#hostname R1* *R1(config)#*
Contraseña de exec privilegiado cifrada	***class*** *R1(config)#enable secret class*
Contraseña de acceso a la consola	***cisco*** *R1(config)#console 0* *R1(config-line)#password cisco* *R1(config-line)#login* *R1(config-line)#exit*
Contraseña de acceso Telnet	***cisco*** *R1(config)#line vty 0 5* *R1(config-line)#password cisco* *R1(config-line)#login* *R1(config-line)#exit*
Cifrar las contraseñas de texto no cifrado	*R1(config)#service password-encryption*
Mensaje MOTD	***Se prohíbe el acceso no autorizado.*** *R1(config)#banner motd "#############se prohibe el acceso no autorizado########"* *R1(config)#*

Interfaz S0/0/0	***Establezca la descripción*** *Establecer la dirección IPv4* *R1(config)#interface serial 0/0/0* *R1(config-if)#ip address 172.16.1.1 255.255.255.252* *R1(config-if)#exit* ***Establecer la dirección IPv6*** *R1(config)#ipv6 unicast-routing* *R1(config)#interface serial 0/0/0* *R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64* ***Establecer la frecuencia de reloj en 128000*** *R1(config-if)#clock rate 128000* ***Activar la interfaz*** *R1(config-if)#no shutdown*
Rutas predeterminadas	***Configurar una ruta IPv4 predeterminada de S0/0/0*** *R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 (la segunda dirección de red Ipv4)* ***Configurar una ruta IPv6 predeterminada de S0/0/0*** *R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2* *(la segunda dirección de red Ipv6)*

Nota: Todavía no configure G0/1.

5.4.3 Paso 3. Configurar R2.

La configuración del R2 incluye las siguientes tareas:

Tabla 4 configuración del R2

Elemento o tarea de configuración	*Especificación*
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	***R2*** *Router(config)#hostname R2* *R2(config)#*
Contraseña de exec privilegiado cifrada	***class*** *R2(config)#enable secret class*
Contraseña de acceso a la consola	*cisco* *R2(config)#console 0* *R2(config-line)#password cisco* *R2(config-line)#login* *R2(config-line)#exit*
Contraseña de acceso Telnet	***cisco*** *R2(config)#line vty 0 5* *R2(config-line)#password cisco* *R2(config-line)#login* *R2(config-line)#exit*
Cifrar las contraseñas de texto no cifrado	*R2(config)#service password-encryption* *R2(config)#exit*
Habilitar el servidor HTTP	*R2(config)#ip http server* *R2(config)#ip http secure-server* *R2(config)#ip http authentication local*
Mensaje MOTD	***Se prohíbe el acceso no autorizado****.* *R2(config)#banner motd "#############se prohibe el acceso no autorizado########"* *R2(config)#*

5.4.4 Paso 4. Configurar R3.

La configuración del R3 incluye las siguientes tareas:

Tabla 5 configuración del R3

Elemento o tarea de configuración	***Especificación***
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	***R3*** *Router(config)#hostname R3* *R3(config)#*
Contraseña de exec privilegiado cifrada	***class*** *R3(config)#enable secret class*
Contraseña de acceso a la consola	***cisco*** *R3(config)#console 0* *R3(config-line)#password cisco* *R3(config-line)#login* *R3(config-line)#exit*
Contraseña de acceso Telnet	***cisco*** *R3(config)#line vty 0 5* *R3(config-line)#password cisco* *R3(config-line)#login* *R3(config-line)#exit*
Cifrar las contraseñas de texto no cifrado	*R3(config)# service password-encryption*
Mensaje MOTD	*Se prohíbe el acceso no autorizado.* *R3(config)#banner motd "############se prohibe el acceso no autorizado#########"* *R3(config)#*
Interfaz S0/0/1	***Establecer la descripción*** ***Establezca la dirección IPv4.*** *(siguiente dirección disponible en la subred.)* *R3(config)#interface serial 0/0/1* *R3(config-if)#ip address 172.16.2.1 255.255.255.252*

	R3(config-if)#exit ***Establezca la dirección IPv6.*** *R3(config)#ipv6 unicast-routing* *R3(config)#interface serial 0/0/1* *R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64* *R3(config-if)#exit* ***Activar la interfaz*** *R3(config-if)#no shutdown*
Interfaz loopback 4	***Establezca la dirección IPv4.*** *(la primera dirección disponible en la subred.)* *R3(config)#interface loopback 4* *R3(config-if)#ip address 192.168.4.1 255.255.255.0* *R3(config-if)#exit*
Interfaz loopback 5	***Establezca la dirección IPv4.*** *(primera dirección disponible en la subred.)* *R3(config)#interface loopback 5* *R3(config-if)#ip address 192.168.5.1 255.255.255.0* *R3(config-if)#exit*
Interfaz loopback 6	***Establezca la dirección IPv4.*** *(primera dirección disponible en la subred.)* *R3(config)#interface loopback 6* *R3(config-if)#ip address 192.168.6.1 255.255.255.0* *R3(config-if)#exit*
Interfaz loopback 7	***Establezca la dirección IPv6.*** *R3(config)#interface loopback 7* *R3(config-if)#ip address 192.168.7.1 255.255.255.0* *R3(config-if)#exit*
Rutas predeterminadas	

5.4.5 Paso 5. Configurar S1.

La configuración del S1 incluye las siguientes tareas:

Tabla 6 configuración del S1

Elemento o tarea de configuración	***Especificación***
Desactivar la búsqueda DNS	*Switch(config)#no ip domain-lookup*
Nombre del switch	***S1*** *Switch(config)#hostname S1* *S1(config)#*
Contraseña de exec privilegiado cifrada	***class*** *class* *S1(config)#enable secret class*
Contraseña de acceso a la consola	***cisco*** *S1(config)#line console 0* *S1(config-line)#password cisco* *S1(config-line)#login* *S1(config-line)#exit*
Contraseña de acceso Telnet	***cisco*** *S1(config)#line vty 0 5* *S1(config-line)#password cisco* *S1(config-line)#login* *S1(config-line)#exit*
Cifrar las contraseñas de texto no cifrado	*S1(config)#service password-encryption* *S1(config)#exit*
Mensaje MOTD	***Se prohíbe el acceso no autorizado.*** *S1(config)#banner motd #Se prohibe el acceso no autorizado#* *S1(config)#exit*

5.4.6 Paso 6. Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

Tabla 7 configuración del S3

Elemento o tarea de configuración	*Especificación*
Desactivar la búsqueda DNS	
Nombre del switch	***S3*** *Switch(config)#hostname S3* *S3(config)#*
Contraseña de exec privilegiado cifrada	***class*** *S3(config)#enable secret class*
Contraseña de acceso a la consola	***cisco*** *S3(config)#line console 0* *S3(config-line)#password cisco* *S3(config-line)#login* *S3(config-line)#exit*
Contraseña de acceso Telnet	***cisco*** *S3(config-line)#line vty 0 5* *S3(config-line)#password cisco* *S3(config-line)#login* *S3(config-line)#exit*
Cifrar las contraseñas de texto no cifrado	*S3(config)#service password-encryption* *S3(config)#exit*
Mensaje MOTD	***Se prohíbe el acceso no autorizado.*** *S3(config)#banner motd #Se prohibe el acceso no autorizado#* *S3(config)#exit* *S3#login*

5.4.7 Paso 7. Verificar la conectividad de la red.

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

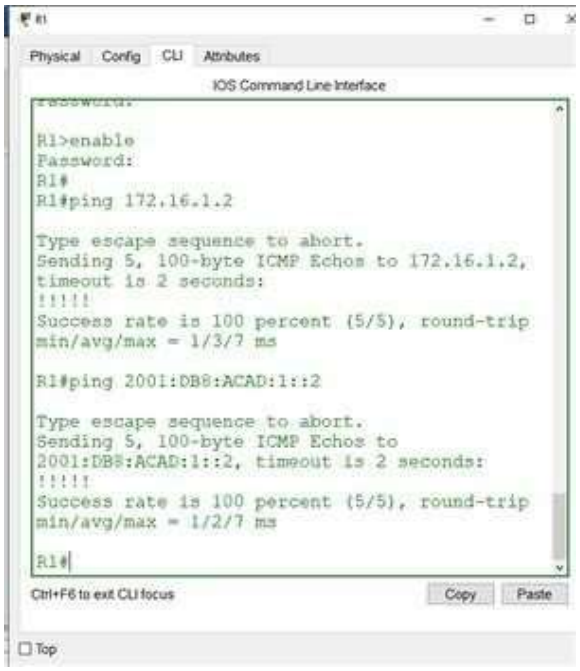
Tabla 8 verificar metódicamente la conectividad con cada dispositivo de red.

Desde	A	*Dirección IP*	*Resultados de ping*
R1	R2, S0/0/0	*172.16.1.2* *2001:DB8:ACAD:1::2*	*sucessful*
R2	R3, S0/0/1	*172.16.2.1* *2001:DB8:ACAD:2::1*	*sucessful*
PCA de Internet	Gateway predeterminado	*192.168.21.1*	*sucessful*

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

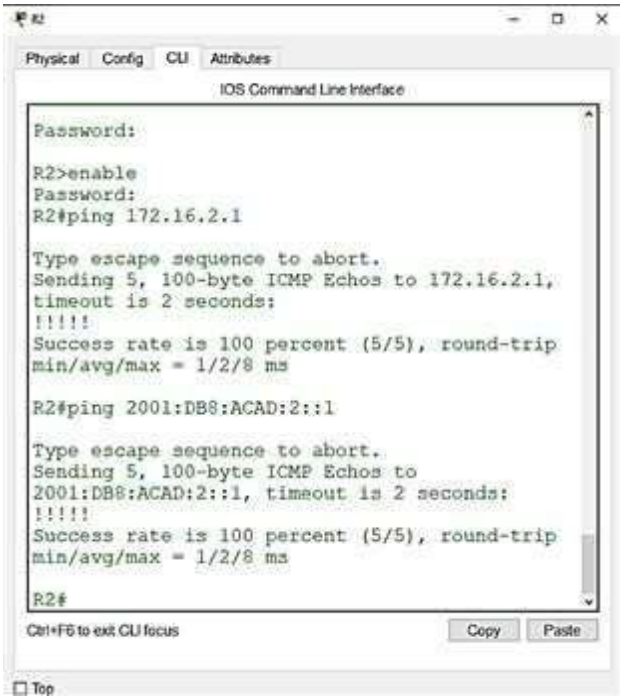
5.5 R1 A R2, S0/0/0

Figura 2 CLI



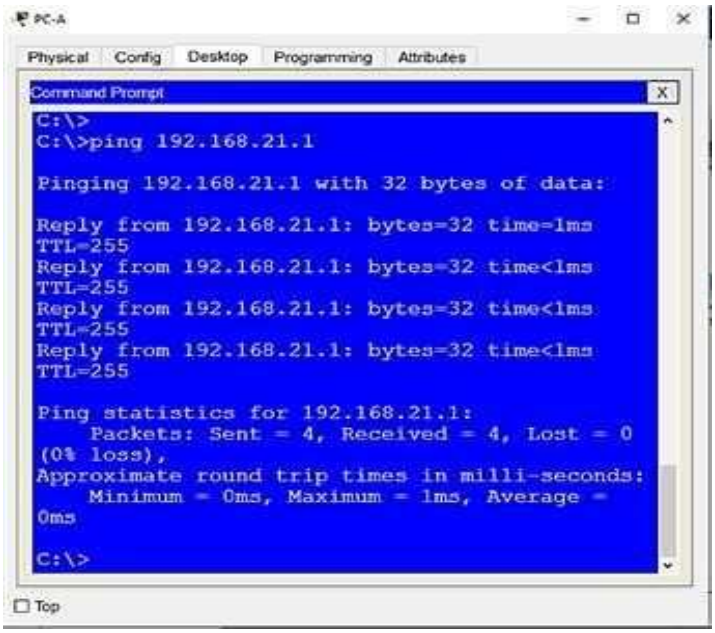
5.5.1 R2 A R3, S0/0/1

Figura 3 CU



5.5.2 PC A de Internet a Gateway predeterminado.

Figura 4 Desktop



5.6 Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

5.6.1 Paso 1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 configuración del S1

Elemento o tarea de configuración	*Especificación*
Crear la base de datos de VLAN	***las VLAN que se indican*** ***Contabilidad*** *S1(config)#vlan 21* *S1(config-vlan)#name Contabilidad* ***Ingeniería*** *S1(config-vlan)#vlan 23* *S1(config-vlan)#name Ingenieria* ***Administración*** *S1(config-vlan)#vlan 99* *S1(config-vlan)#name Administracion*
Asignar la dirección IP de administración.	***Asigne la dirección IPv4 a la VLAN de administración*** *(Utilizar la dirección IP asignada al S1)* *S1(config)#interface vlan 99* *S1(config-if)#ip address 192.168.99.2 255.255.255.0*
Asignar el Gateway predeterminado	***Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado****.* *S1(config)#ip default-gateway 192.168.99.1*

Forzar el enlace troncal en la interfaz F0/3	***Utilizar la red VLAN 1 como VLAN nativa*** *S1(config)#interface F0/3* *S1(config-if)#switchport mode trunk* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#exit*
Forzar el enlace troncal en la interfaz F0/5	***Utilizar la red VLAN 1 como VLAN nativa*** *S1(config)#interface F0/5* *S1(config-if)#switch mode trunk* *S1(config-if)#switchport trunk native vlan 1* *S1(config-if)#exit*
Configurar el resto de los puertos como puertos de acceso.	***Utilizar el comando interface range*** *S1(config)#interface range F0/1-2, F0/4, F0/6-24* *S1(config-if-range)#switchport mode access* *S1(config-if-range)#exit*
Asignar F0/6 a la VLAN 21	*S1(config)#interface F0/6* *S1(config-if)#switchport access vlan 21*
Apagar todos los puertos sin usar	*S1(config)#interface range F0/1-2, F0/4, F0/7-24* *S1(config-if-range)#shutdown*

5.6.2 Paso 2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10 configuración del S3

Elemento o tarea de configuración	*Especificación*
Crear la base de datos de VLAN	*crear cada una de las VLAN que se indican Dé nombre a cada VLAN.* ***contabilidad*** *S3(config)#vlan 21* *S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23* ***Ingeniería*** *S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99* ***administración*** *S3(config-vlan)#name Administracion*
Asignar la dirección IP de administración	*Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología* *S3(config)#interface vlan 99* *S3(config-if)#ip address 192.168.99.3 255.255.255.0* *S3(config-if)#exit*
Asignar el Gateway predeterminado.	*Asignar la primera dirección IP en la subred como Gateway predeterminado.* *S3(config)#ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	*Utilizar la red VLAN 1 como VLAN nativa* *S3(config)#interface F0/3* *S3(config-if)#switchport mode trunk* *S3(config-if)#switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	*Utilizar el comando interface range* *S3(config)#interface range F0/1-2, F0/4-24* *S3(config-if-range)#switchport mode access*
Asignar F0/18 a la VLAN 21	*S3(config)#interface F0/18* *S3(config-if)#switchport access vlan 21*

Apagar todos los puertos sin usar	*S3(config)#interface range F0/1-2, F0/4-17, F0/19-24* *S3(config-if-range)#shutdown*

5.6.3 Paso 3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 tareas de configuración para R1

Elemento o tarea de configuración	***Especificación***
Configurar la subinterfaz 802.1Q .21 en G0/1	***Descripción: LAN de Contabilidad*** ***Asignar la VLAN 21*** *(la primera dirección disponible a esta interfaz)* *R1(config)#interface G0/1.21* *R1(config-subif)#description accounting LAN* *R1(config-subif)#encapsulation dot1q 21* *R1(config-subif)#ip address 192.168.21.1 255.255.255.0* *R1(config-subif)#exit*
Configurar la subinterfaz 802.1Q .23 en G0/1	***Descripción: LAN de Ingeniería*** ***Asignar la VLAN 23*** *(la primera dirección disponible a esta interfaz)* *R1(config)#interface G0/1.23* *R1(config-subif)#description accounting LAN* *R1(config-subif)#encapsulation dot1q 23* *R1(config-subif)#ip address 192.168.23.1 255.255.255.0* *R1(config-subif)#exit*

Configurar la subinterfaz 802.1Q .99 en G0/1	*Descripción: LAN de Administración* *Asignar la VLAN 99* *(la primera dirección disponible a esta interfaz)* *R1(config)#interface G0/1.99* *R1(config-subif)#description accounting LAN* *R1(config-subif)#encapsulation dot1q 99* *R1(config-subif)#ip address 192.168.99.1 255.255.255.0* *R1(config-subif)#exit*
Activar la interfaz G0/1	*R1(config)#interface G0/1* *R1(config-if)#no shutdown* *R1(config-subif)#exit*

5.6.4 Paso4. Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12 para verificar metódicamente la conectividad con cada dispositivo de red.

Desde	A	*Dirección IP*	*Resultados de ping*
S1	R1, dirección VLAN 99	*192.168.99.1*	*succesful*
S3	R1, dirección VLAN 99	*192.168.99.1*	*succesful*
S1	R1, dirección VLAN 21	*192.168.21.1*	*succesful*
S3	R1, dirección VLAN 23	*192.168.23.1*	*succesful*

5.7 Parte 4. Configurar el protocolo de routing dinámico RIPv2

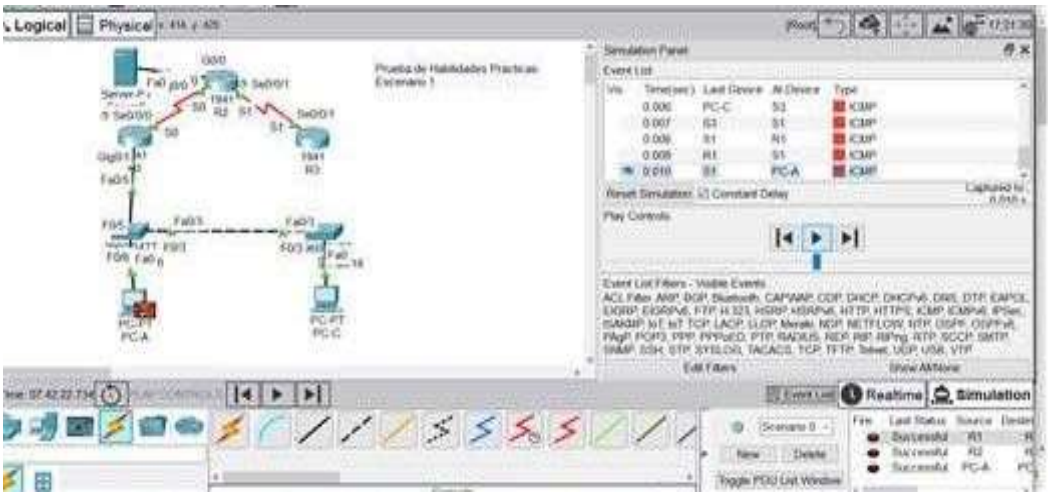


Figura 5 Configurar el protocolo de routing dinámico RIPv2

5.7.1 Paso 1. Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Ilustración 6 Tareas de configuración para R1

Elemento o tarea de configuración	***Especificación***
Configurar RIP versión 2	*R1(config)#router rip* *R1(config-router)#version 2* *R1(config-router)#exit*
Anunciar las redes conectadas directamente	*Asigne todas las redes conectadas directamente* *R1(config-router)#network 172.16.1.0* *R1(config-router)#network 192.168.99.0* *R1(config-router)#exit*
Establecer todas las interfaces LAN como pasivas	*R1(config-router)#passive-interface default*
Desactive la sumarización automática	*R1(config-router)#no auto-summary*

5.7.2 Paso 2. Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 13 configuración del R2

Elemento o tarea de configuración	***Especificación***
Configurar RIP versión 2	*R2(config)#router rip* *R2(config-router)#version 2*
Anunciar las redes conectadas directamente	***Nota:*** *Omitir la red G0/0.* *R2(config-router)#network 172.16.1.0* *R2(config-router)#network 172.16.2.0*
Establecer la interfaz LAN (loopback) como pasiva	*R2(config-router)#passive-interface loopback 0*
Desactive la sumarización automática.	*R2(config-router)#no auto-summary*

5.7.3 Paso 3. Configurar RIPv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 14 Tareas para la configuración del R3

Elemento o tarea de configuración	***Especificación***
Configurar RIP versión 2	*R3(config)#router rip* *R3(config-router)#version 2*
Anunciar redes IPv4 conectadas directamente	*R3(config-router)#network 172.16.2.0*
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	*R3(config-router)#passive-interface loopback 4* *R3(config-router)#passive-interface loopback 5* *R3(config-router)#passive-interface loopback 6*

Desactive la sumarización automática.	*R3(config-router)#no auto-summary*

5.7.4 Paso4. Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 15 Verificación RIP

Pregunta	***Respuesta***
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	*R1#show ip protocols*
¿Qué comando muestra solo las rutas RIP?	*R1#show ip rip database*
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	*R1#show running-config*

5.8 Parte 6. Implementar DHCP y NAT para IPv4

5.8.1 Paso1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 tareas de configuración para R1

Elemento o tarea de configuración	***Especificación***
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	*R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20* *R1(config)#exit*
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	*R3(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20* *R3(config)#exit*

Crear un pool de DHCP para la VLAN 21.	*Nombre: ACCT* *Servidor DNS: 10.10.10.10* *Nombre de dominio: ccna-sa.com* *Establecer el Gateway predeterminado* *R1(dhcp-config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com* *R1(dhcp-config)#default-router 192.168.21.1* *R1(dhcp-config)#exit* *R1(dhcp)#*
Crear un pool de DHCP para la VLAN 23	*Nombre: ENGNR* *Servidor DNS: 10.10.10.10* *Nombre de dominio: ccna-sa.com* *Establecer el gateway predeterminado* *R3(dhcp-config)#ip dhcp pool ACCT R3(dhcp-config)#dns-server 10.10.10.10 R3(dhcp-config)#domain-name ccna-sa.com* *R3(dhcp-config)#default-router 192.168.21.1* *R3(dhcp-config)#exit* *R3(dhcp)#*

5.8.2 Paso 2. Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17 Tareas de configuración del R2

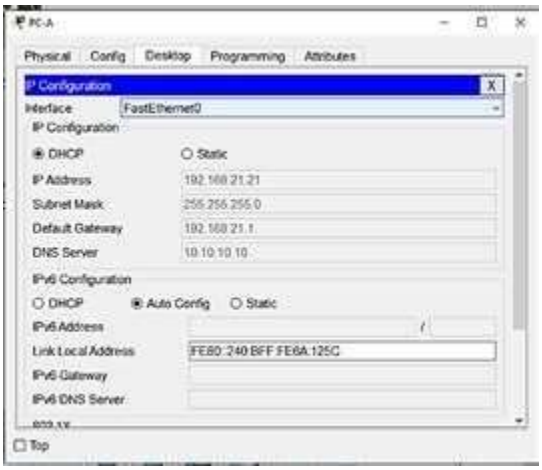
Elemento o tarea de configuración	***Especificación***
Crear una base de datos local con una cuenta de usuario	*Nombre de usuario:* ***webuser*** *Contraseña:* ***cisco12345*** *Nivel de privilegio:* ***15*** *R2(config)#user webuser privilege 15 secret cisco12345*
Habilitar el servicio del servidor HTTP	*R2(config)#ip http server*
Configurar el servidor	*R2(config)#ip http autentication local*

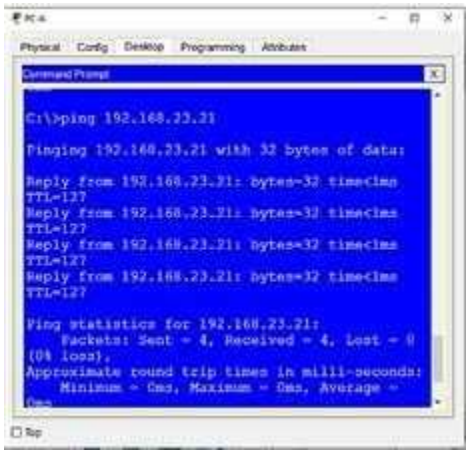
HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	***Dirección global interna: 209.165.200.229*** *R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229* *R2(config)#exit*
Asignar la interfaz interna y externa para la NAT estática	*R2(config)#interface G0/1 R2(config-if)#ip nat outside R2(config-if)#interface G0/0* *R2(config-if)#ip nat inside* *R2(config-if)#ip nat inside* *R2(config)#exit*
Configurar la NAT dinámica dentro de una ACL privada	*Lista de acceso: 1* *Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1* *Permitir la traducción de un resumen de las redes LAN (loopback) en el R3* *R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255* *R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255* *R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255* *R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255* *R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255* *R2(config)#exit*
Defina el pool de direcciones IP públicas utilizables.	*Nombre del conjunto:* ***INTERNET*** *El conjunto de direcciones incluye:* ***209.165.200.225*** *–* ***209.165.200.228*** *R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248* *R2(config)#exit*
Definir la traducción de NAT dinámica	*R2(config)#ip nat inside source list 1 pool INTERNET*

5.8.3 Paso 3. Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 18 configuraciones de DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Esta configuración es posible desde equipo telnet a un pc En el simulador no es posible realizar algunos comandos.

5.9 Parte 6. Configurar NTP

Tabla 19 Configurar NTP

Elemento o tarea de configuración	***Especificación***
Ajuste la fecha y hora en R2.	***5 de marzo de 2016, 9 a. m.*** *R2#clock set 09:00:00 5 mar 2016* *R2#exit*
Configure R2 como un maestro NTP.	***Nivel de estrato: 5*** *R2(config)#ntp master 5* *R2(config)#*
Configurar R1 como un cliente NTP.	***Servidor: R2*** *R1(config)#ntp server 172.16.1.2* *R1(config)#*

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	*R1(config)#ntp update-Calendar* *R1(config)#*
Verifique la configuración de NTP en R1.	*R1#show ntp Associations* *R1#*

5.10 Parte 7. Configurar y verificar las listas de control de acceso (ACL)

5.10.1 Paso 1. Restringir el acceso a las líneas VTY en el R2.

Tabla 20 Restringir el acceso a las líneas VTY en el R2.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 5 R2(config-line)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN in
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

5.10.2 Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 21 Introducir el comando de CLI

Descripción del comando	***Entrada del estudiante (comando)***
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	*R2#show access-list*
Restablecer los contadores de una lista de acceso	*R2(config)#no access-list 10*

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*R2#show access-list 1*
¿Con qué comando se muestran las traducciones NAT?	***Nota:*** *Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.* *R2#show ip nat translations*
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*R2#clear ip nat translation **

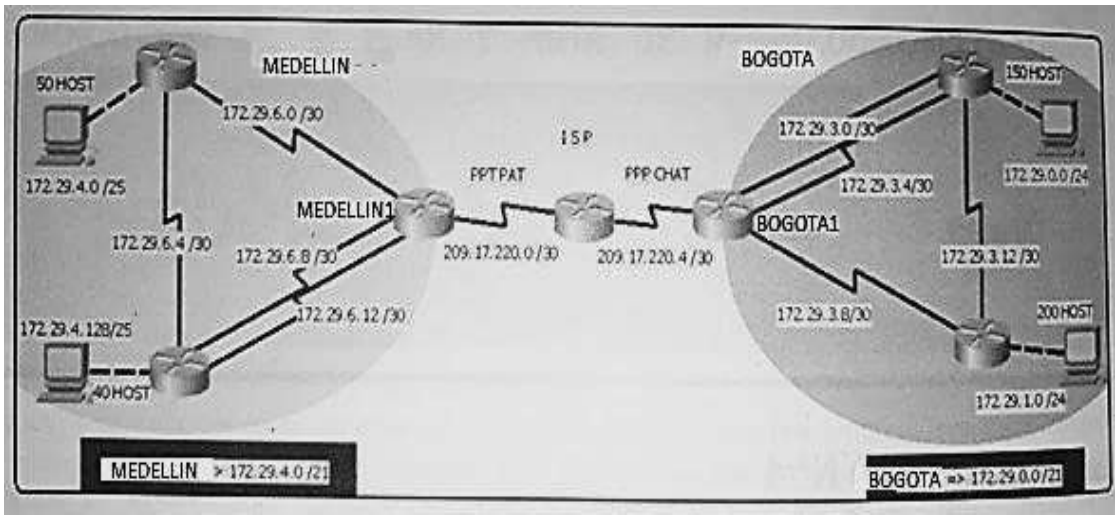
6 DESARROLLO ESCENARIO 2.

6.2 Escenario 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

6.3 Topología de red

Figura 7Tipología de red escenario 2



Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación. Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

6.3.1 Desarrollo.

Como trabajo inicial se debe realizar lo siguiente:

a. Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.).

b. Realizar la conexión física de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

6.3.2 Topología de la red sin conectividad

Figura 8 Topología de la red sin conectividad

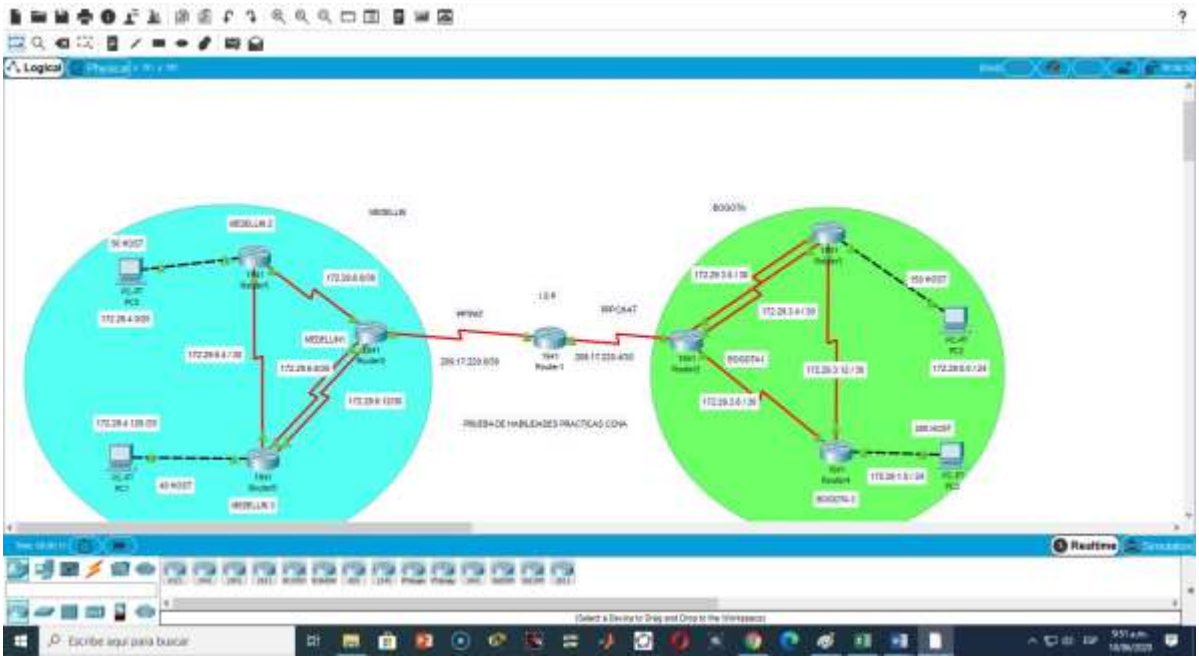


Tabla 22 Tabla de direccionamiento

Device	Interface	Ip Address	Subnet Mask	gateway
Medellin1	S0/1/1	209.17.220.1	255.255.255.252	209.17.220.0
	S0/0/1	172.29.6.1	255.255.255.252	172.29.6.0
	S0/0/0	172.29.6.9	255.255.255.252	172.29.6.8
Device	S0/1/0	172.29.6.13	255.255.255.252	172.29.6.12
Medellin2	S0/0/1	172.29.6.2	255.255.255.252	172.29.6.0
	S0/0/0	172.29.6.5	255.255.255.252	172.29.6.4
	G0/0	172.29.4.1	255.255.255.128	172.29.4.0
Medellin3	S0/0/0	172.29.6.6	255.255.255.252	172.29.6.4
	S0/0/1	172.29.6.10	255.255.255.252	172.29.6.8

	S0/1/0	172.29.6.13	255.255.255.252	172.29.6.12
	gG0/0	172.29.4.129	255.255.255.128	172.29.4.128
ISP	S0/0/0	209.17.220.2	255.255.255.252	209.17.220.0
	S0/0/1	209.17.220.5	255.255.255.252	209.17.220.4
Bogota1	S0/1/1	172.29.3.1	255.255.255.252	172.29.3.0
	S0/1/1	172.29.3.5	255.255.255.252	172.29.3.4
	S0/1/1	172.29.3.9	255.255.255.252	172.29.3.8
Bogota2	S0/1/1	172.29.3.2	255.255.255.252	172.29.3.0
	S0/1/1	172.29.3.6	255.255.255.252	172.29.3.4
	S0/1/1	172.29.3.13	255.255.255.252	172.29.3.12
	G0/0	172.29.0.1	255.255.255.0	172.29.0.0
Bogota3	S0/1/1	172.29.3.10	255.255.255.252	172.29.3.8
	S0/1/1	172.29.3.14	255.255.255.252	172.29.3.12
	g0/0	172.29.1.1	255.255.255.0	172.29.1.0
PC0	nic	172.29.4.0		
PC1	nic	172.29.4.133		
PC2	nic	172.29.0.5		
PC3	nic	172.29.1.4		
PC$	nic			

6.3.3 Configuración básica del Router.

Router>ena

configure terminal

hostname Medellin1

enable secret class

line console 0

pass cisco

login

exit

line vty 0 4

pass cisco

login

exit

service password-encryption

6.3.4 Configuración interfaces

6.3.4.1 Interface s0/1/1

ip address 209.17.220.1 255.255.255.252

no shutdown

exit

6.3.4.2 Interface s0/0/1

ip address 172.29.6.1 255.255.255.252

clock rate 128000

no shutdown

exit

6.3.4.3 Interface s0/0/0

ip address 172.29.6.9 255.255.255.252

no shutdown

exit

6.3.4.4 Interface S0/1/0.

IP address 172.29.6.13 255.255.255.252

clock rate 128000

no shutdown

exit

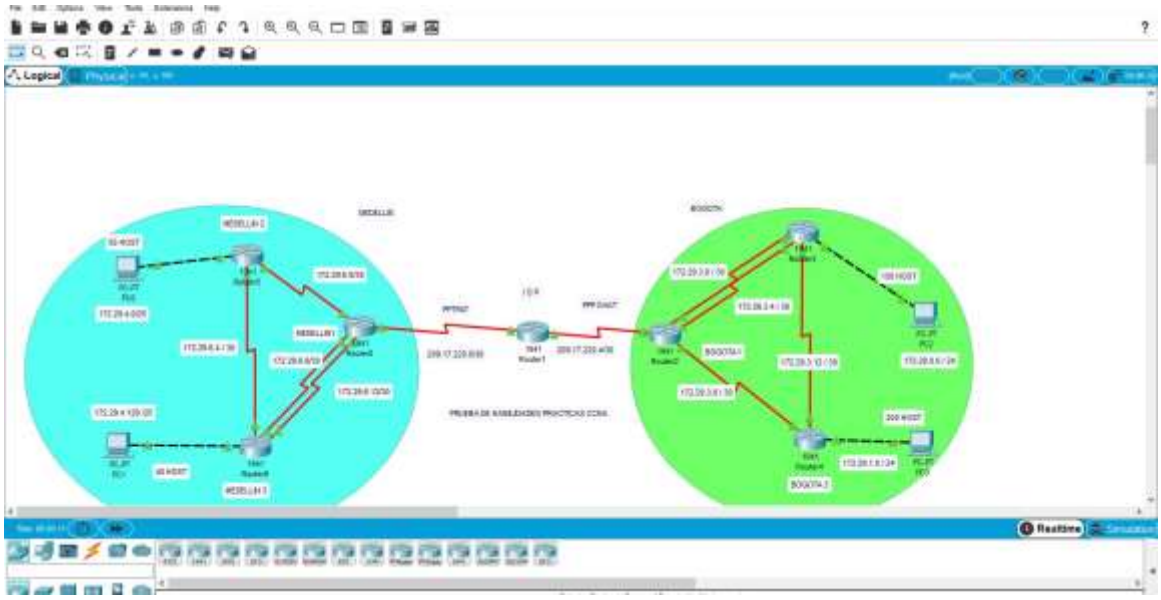
#exit

Wr

Se configura todos los Router de la red escenario 1 según la tabla de direccionamiento y se le asigna la seguridad en los dispositivos.

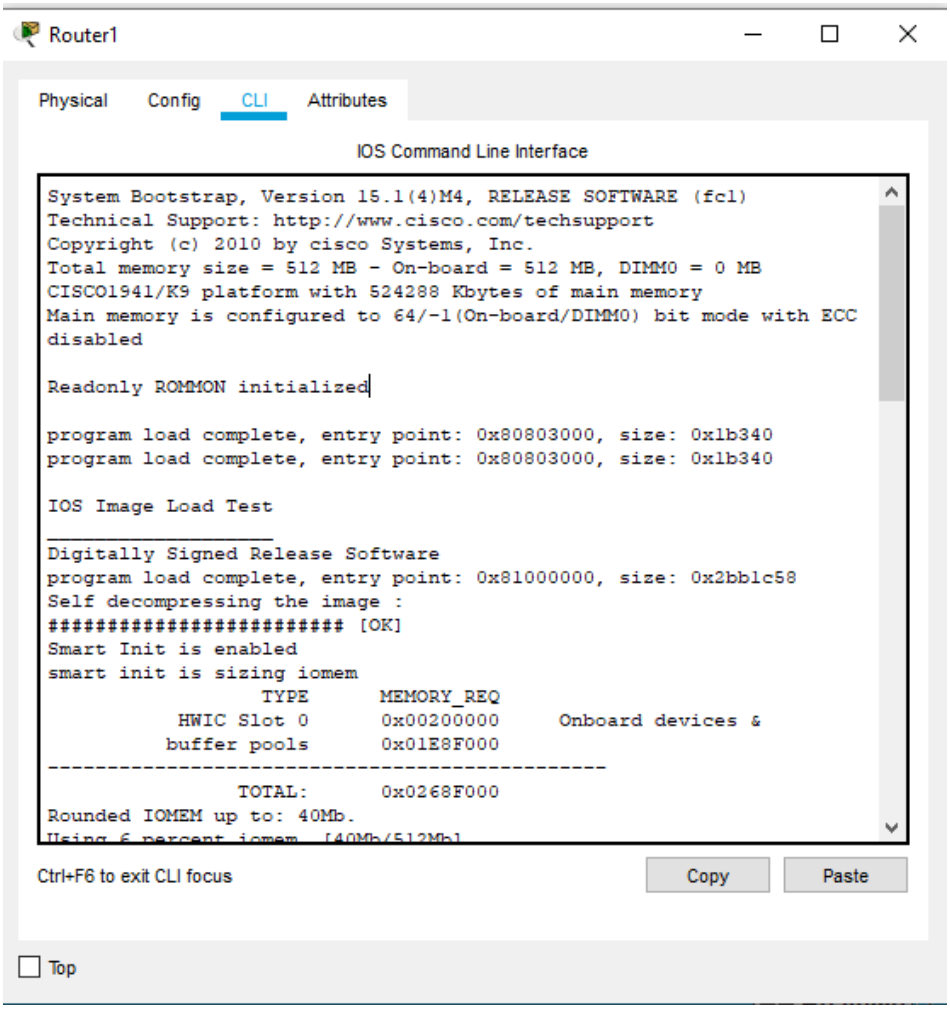
Escenario 1 configurado según la tabla de direccionamiento, hay conectividad entre los routers, pero no se ha configurado para que los dispositivos finales se comuniquen entre ellos. De extremo a extremo.

Figura 9 Escenario 2



La efectividad de la conectividad depende de las redes WAN, pero la conexión de los dispositivos solo ser vera comunicada entre las LAN.

Figura 10 Router1



6.4 Parte 1: Configuración del enrutamiento.

a) **Configurar el enrutamiento en la red usando el protocolo RIP versión 2, declare la red principal, desactive la sumarización automática.**

6.4.1 Configuration Router Rip

- M**edellin2**

enable
configure terminal
router rip
network 172.29.6.0
network 172.29.6.4
network 172.29.4.0
version 2
no auto-summary
exit
exit
wr

- **Medellin3**

enable
configure terminal
router rip
network 172.29.6.4
network 172.29.6.8
network 172.29.6.12
network 172.29.4.128

version 2
no auto-summary
exit
exit
wr

- **Bogotá2**

enable
configure terminal
router rip
network 172.29.3.0
network 172.29.3.4
network 172.29.3.12
network 172.29.0.0
version 2
no auto-summary
exit
exit
wr

- **Bogotá3**

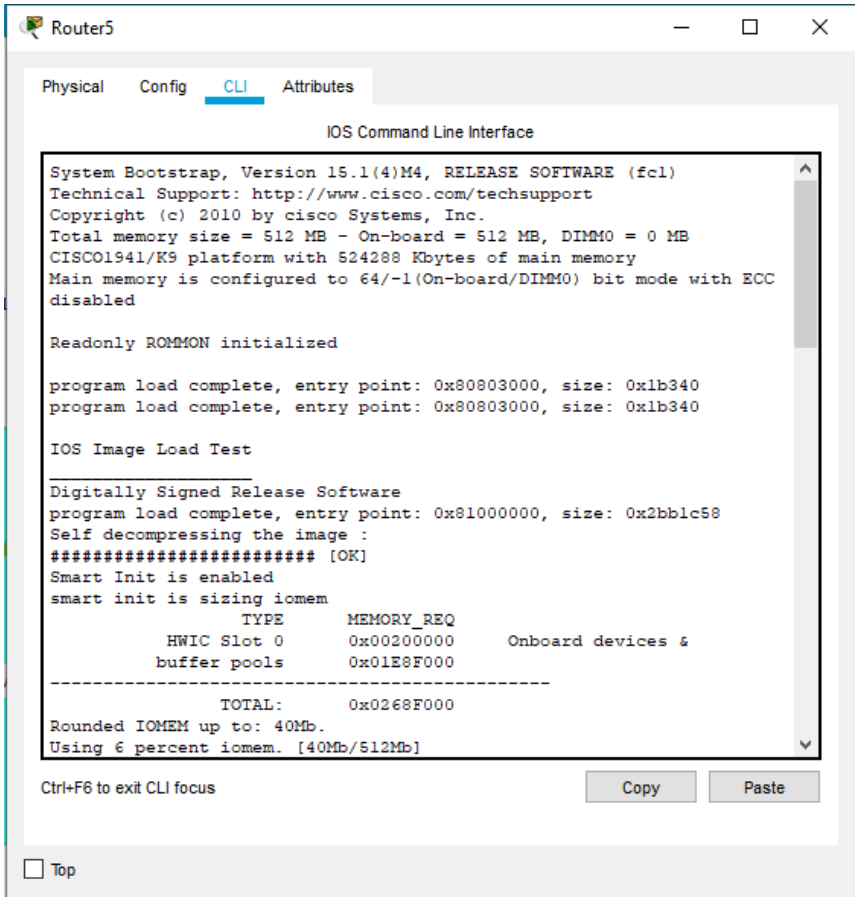
enable
configure terminal
router rip
network 172.29.3.8
network 172.29.3.12
network 172.29.1.0
version 2
no auto-summary

exit

exit

wr

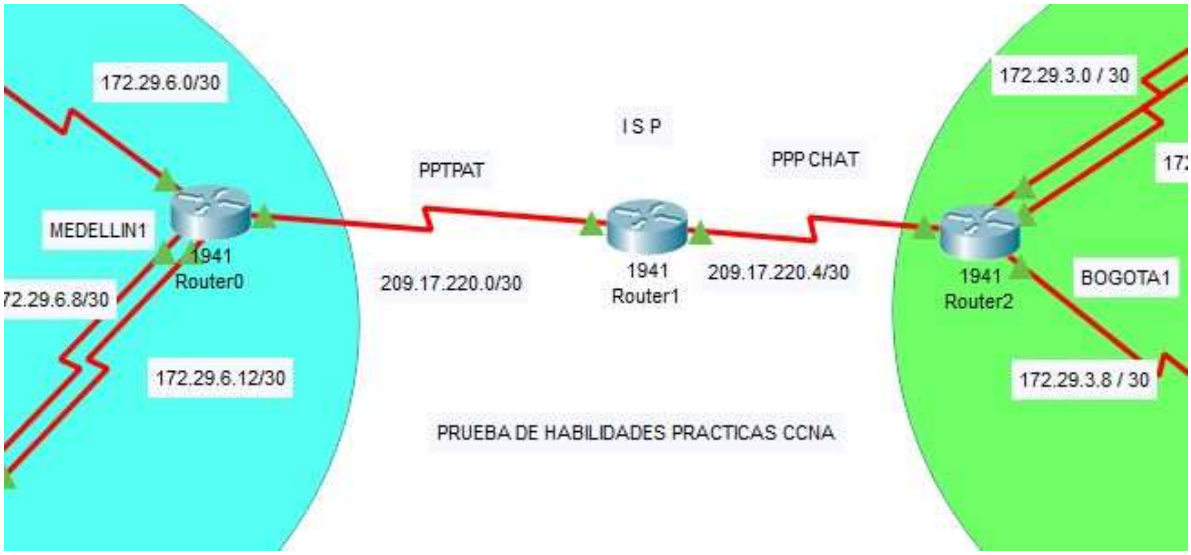
Figura 11 Reuter5



Se asigna la configuración a todos los Router de la red Escenario 1

b) Los routers Bogota1 y Medellín1 deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de RIP.

Figura 12 escenario2



Bogota1

enable

configure terminal

router rip

network 209.17.220.0

network 172.29.3.4

network 172.29.3.8

version 2

no auto-summary

exit

medellin1

enable

configure terminal

router rip

network 209.17.220.0

network 172.29.6.0

network 172.29.6.8

network 172.29.6.12

version 2

no auto-summary

exit

exit

wr

a· El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

ISP

enable

configure terminal

router rip

network 209.17.220.0

network 209.17.220.4

version 2

no auto-summary

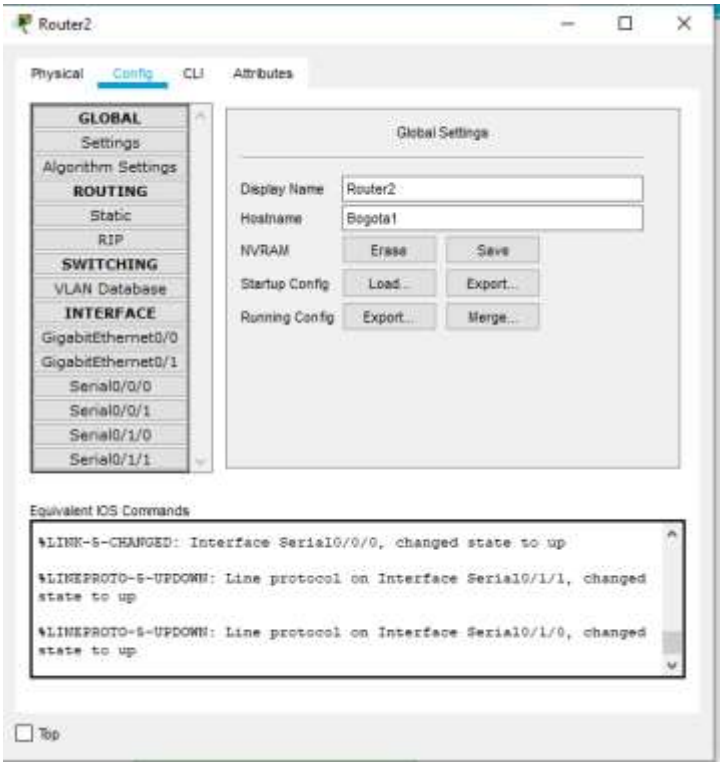
exit

exit

wr

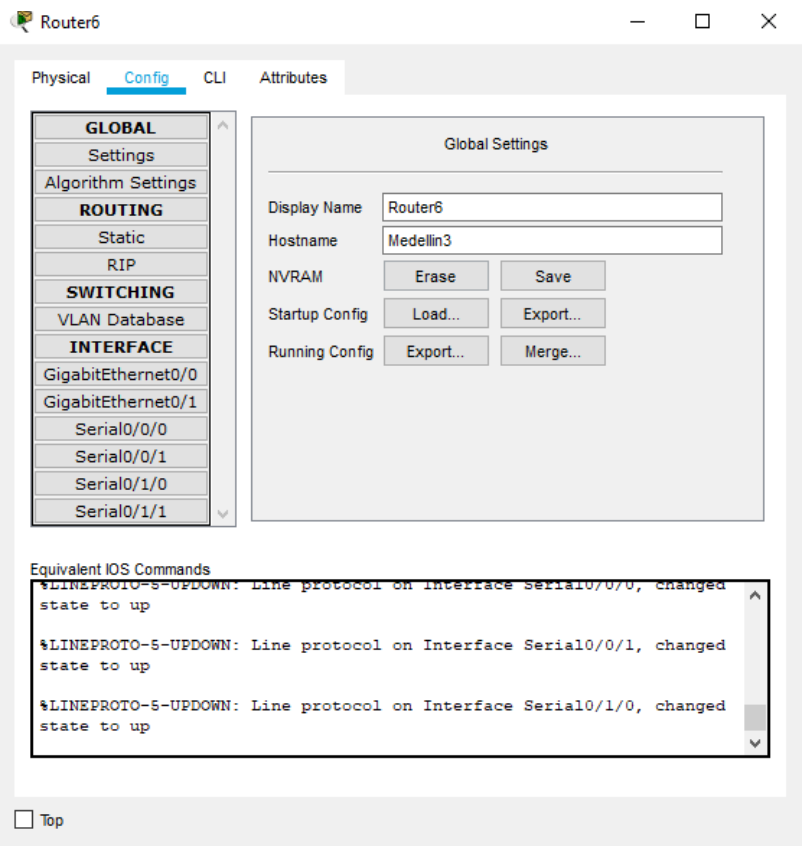
ISP

Figura 13 Router2



- MEDELLIN 1

Figura 14 Router6-Medellin 1



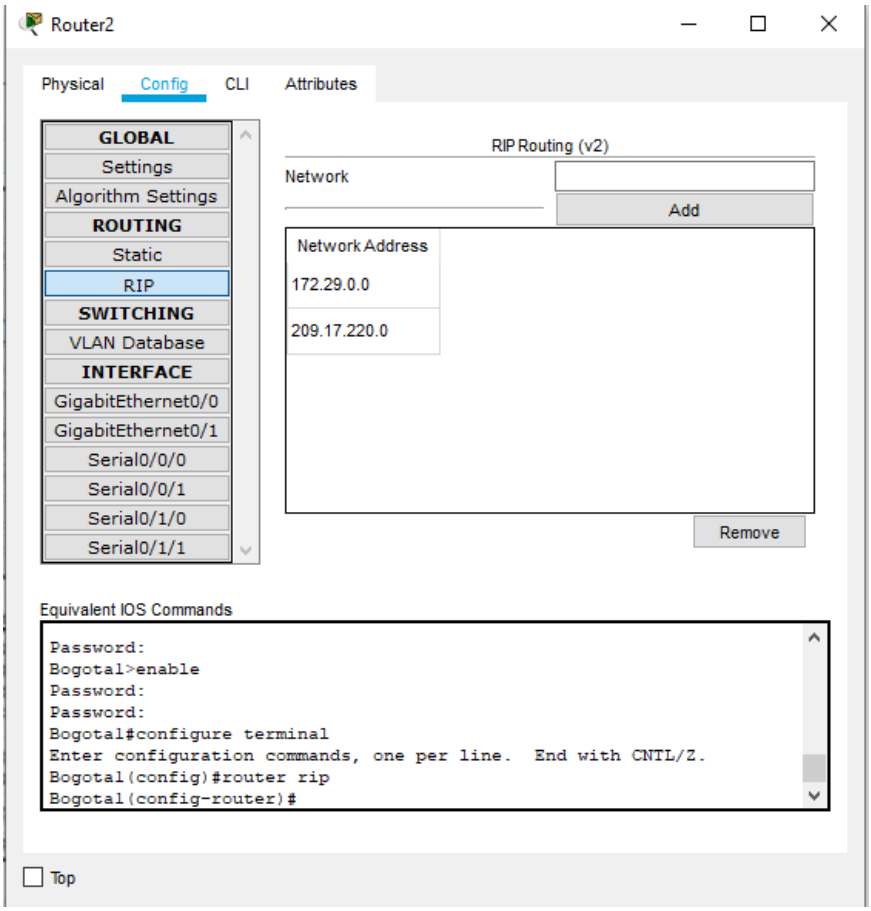
para resumir todas las rutas en una ruta estática. 209.17.220.0 /30; 172.29.6.0/30; 172.29.6.8 /30; 172.29.6.12 /30;

en Router Rip es posible resumir a 172.29.0.0 y 209.12.220.0

y esto sería la ruta resumen

La sumarizacion de las networks optimiza la red mejorando la conectividad y el tráfico de paquetes es mucho más rápido.

Figura 15 Bogotá 1



El mismo caso sucede en Router Bogotá 1

Las rutas configuradas como Rip, 172.29.3.0/30; 172.29.3.4 /30 ; 172.29.3.8 /30 y 209.17.220.6

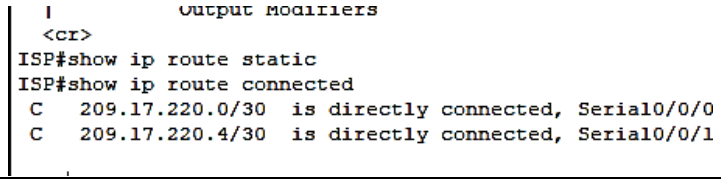
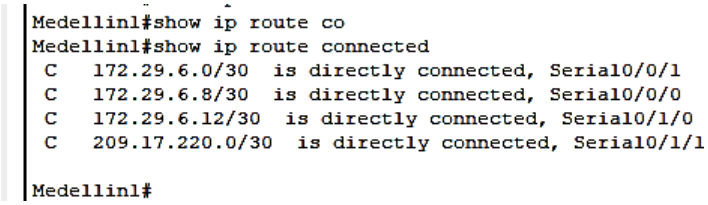
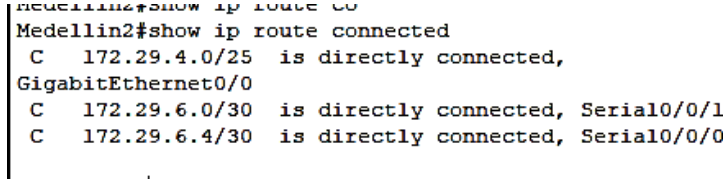
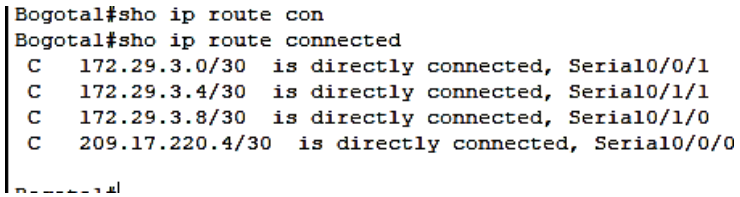
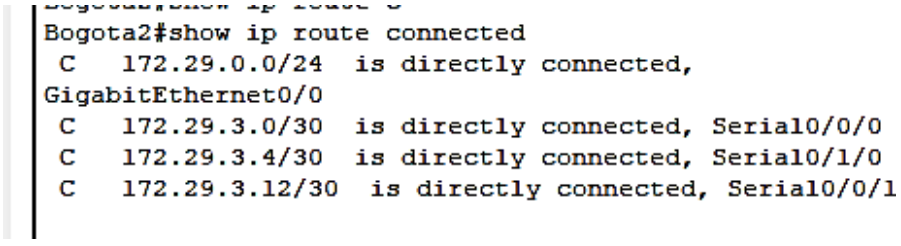
Se ven resumidas en 172.29.0.0 y la 209.17.220.0

6.5 Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

   Comando show ip route connected

Tabla 23Comando show ip route connected

ISP	
Medellin1	
Medellin 2	
Bogota 1	
Bogota 2	

Bogota 3	Bogota3#show ip route c Bogota3#show ip route connected C 172.29.1.0/24 is directly connected, GigabitEthernet0/0 C 172.29.3.8/30 is directly connected, Serial0/0/0 C 172.29.3.12/30 is directly connected, Serial0/0/1 Bogota3#

b· Verificar el balanceo de carga que presentan los routers.

Medellin1

balanceo de carga, comando

show ip route

Router Medellín

Figura 16 Router Medellín

Con este comando podemos verificar el balanceo de carga

En el Route Medellín 1, ambas rutas tienen la misma métrica, a 1 salto

209.17.220.4/30 [120/1] vía 209.17.220.2, 00:00:21, Serial0/1/1

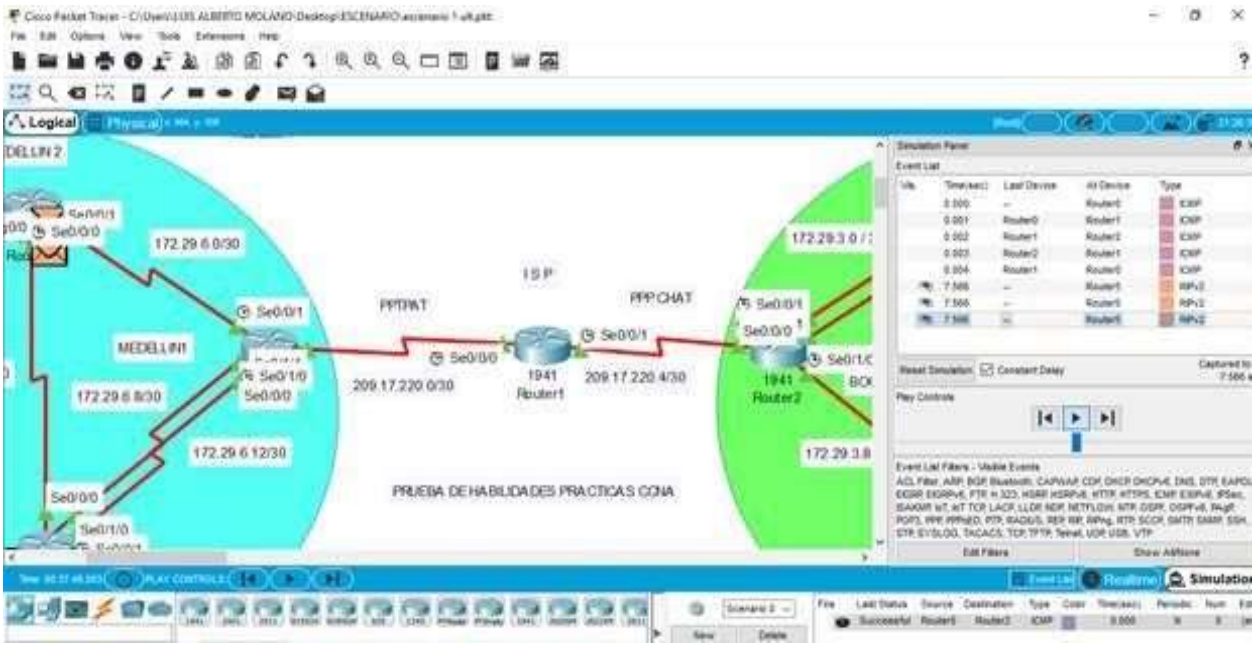
De esta forma podemos verificar cada uno de los Router

La capacidad del Router para transmitir paquetes a un destino de dirección IP está dado por el balanceo de cargas al usar más de una ruta, entre menos ruta mejor balanceo de carga en la red.

c· Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Router Bogotá 1 y Medellín 1 conectado por Route Rip,

Figura 17 Router Bogotá 1 y Medellín 1 conectado por Route Rip,



En esta actividad en la red los Router Medellin1 y Bogota1 hay paquetes enviados, y un ping que se repite a 0.001 time.

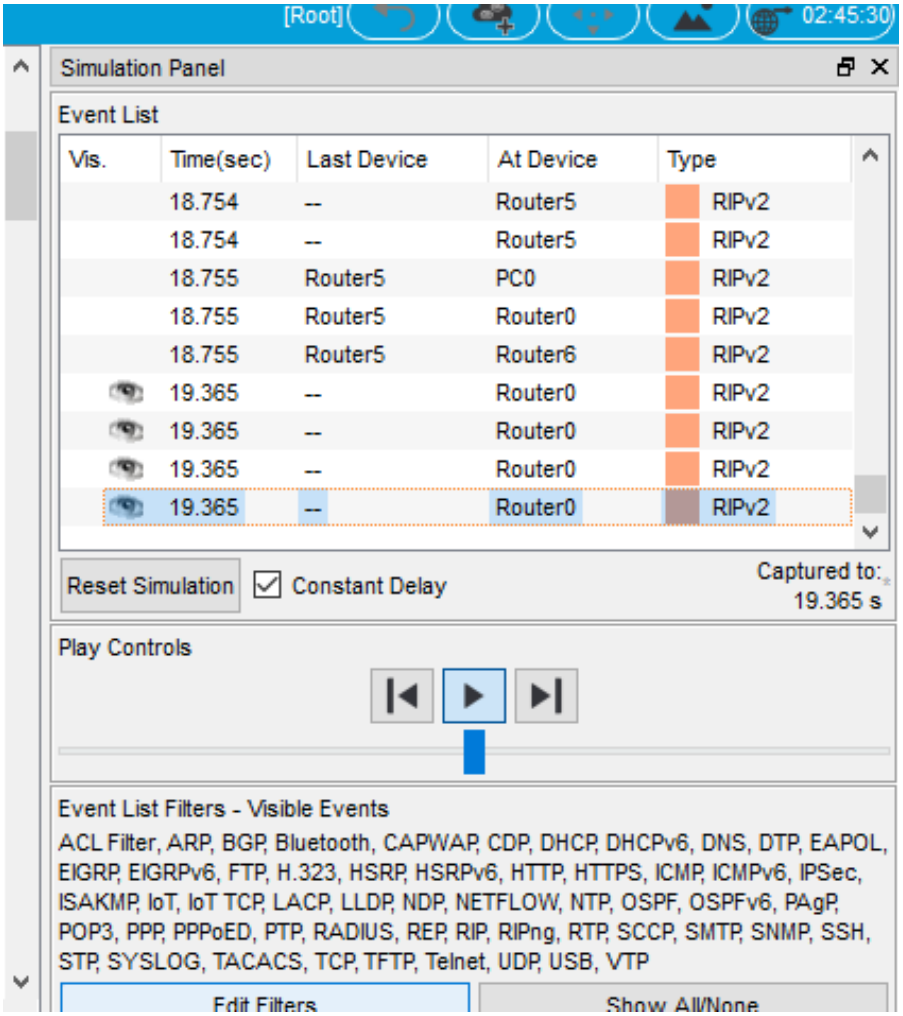
d· Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.

Conectividad Router Rip entre Medellin2 (Router5) y Bogota2 (Router 3)

A los 18.755 time

Type RIPV2

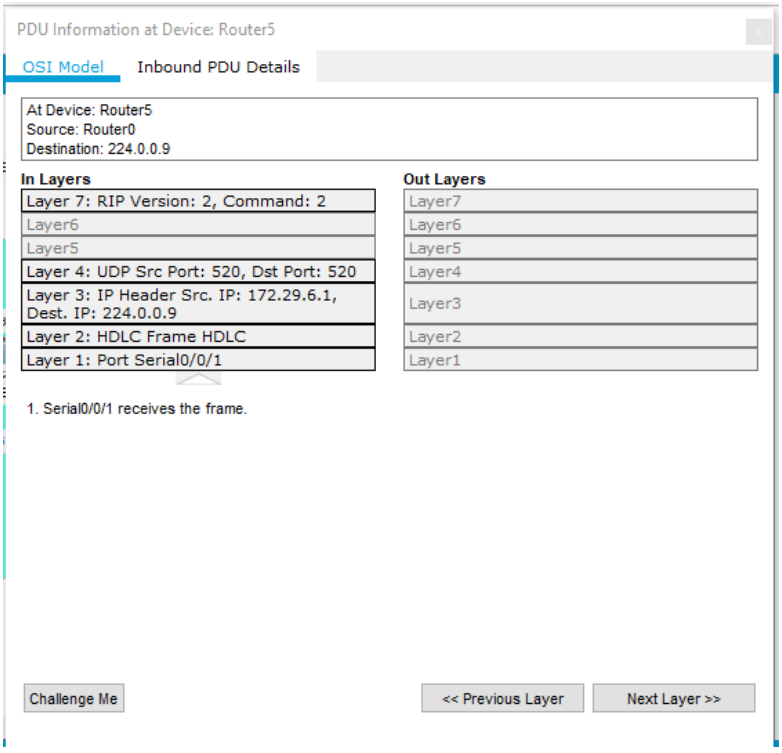
Figura 18 Type RIPV2



Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

La conectividad de Router Medellin2 (Router 5) al Router Medellin1 (Router 0) Tomando rutas por defecto.

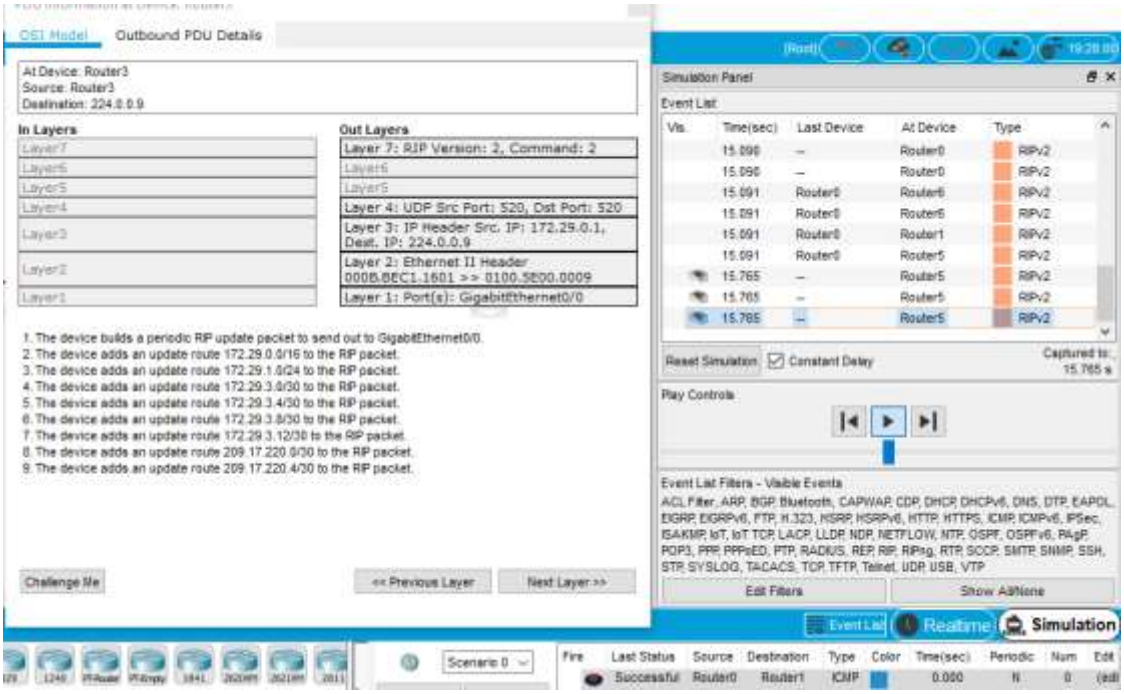
Figura 19 Router Medellin2



El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Router ISP (Router 3)

Figura 20 Router ISP (Router 3)



6.6 Parte 3: Deshabilitar la propagación del protocolo RIP.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo RIP, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 24 interfaces de cada router que no necesitan desactivación.

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1

Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

Route Rip envía mensajes hacia las interfaces conectadas, en las direcciones de red especificadas en la configuración de lista de Route Rip . es necesario administrar la red y para controlar las interfaces de direccionamiento se puede inhabilitar el envió de actualizaciones de las interfaces que sean seleccionadas, usando el comando

Bogota1(config)#router rip

Bogota1(config-router)#pas

Bogota1(config-router)#passive-interface s0/0/1

Bogota1(config-router)#passive-interface s0/1/1

Bogota1(config-router)#passive-interface s0/1/0

Bogota1(config-router)#exit

Bogota1(config)#exit

Esta misma configuración se le asigna a cada uno de los router de escenario 2

Figura 21 Router Bogota2

```
Bogota2(config)#router rip
Bogota2(config-router)#pa
Bogota2(config-router)#passive-interface s0/0/0
Bogota2(config-router)#passive-interface s0/1/0
Bogota2(config-router)#passive-interface s0/0/1
Bogota2(config-router)#exit
Bogota2(config)#exit
Bogota2#
%SYS-5-CONFIG_I: Configured from console by console

Bogota2#
```

6.7 Parte 4: Verificación del protocolo RIP.

a· Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el **passive interface** para la conexión hacia el ISP, la versión de RIP y las interfaces que participan de la publicación entre otros datos.

b. Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

6.8 Parte 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

router(config-router)# ***maximum-paths <número>***

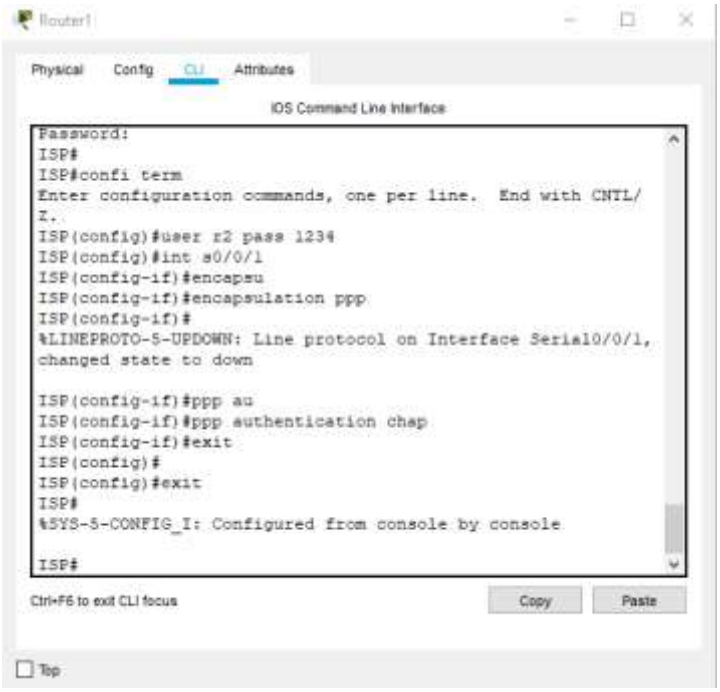
Este comando sirve para cambiar el número máximo de rutas que son permitidas, se debe entrar en el modo Router Rip

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

Figura 22 enlace Bogotá1

La autenticación chap en Router Bogota1 en la interfaz S0/0/1 que conecta con Router ISP le permitirá una conexión más segura en el envío de paquetes, se debe configurar también en Router Isp

Figura 23 Autenticación chap en Router Bogota1



6.9 Parte 6: Configuración de PAT.

a· En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b· Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

c· Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

La configuración Nat

*Bogota1(config)# **ip nad inside source estactic 209.17.220.1 209.17.220.5***

Bogota1(config)# int s0/0/1

Bogota1(config-if)# ip nat outside

Bogota1(config-if)# int s0/0/0

Bogota1(config-if)# ip nat inside

Bogota1(config-if)# exit

6.10 Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

El comando a usar para configurar el Router

Medellín 2

Medellin2(config)# ip address DHCP

Medellin2(config)# EXIT

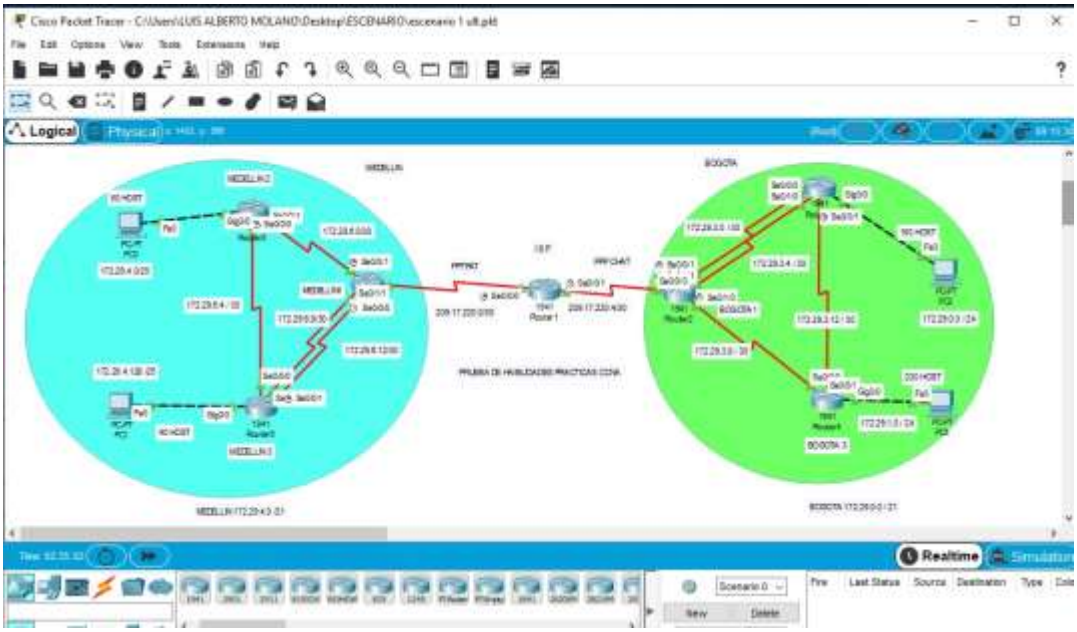
Bogota 2

Bogota2(config)# ip address DHCP

Bogota2(config)# EXIT

6.10.1 Topology de la red escenario 2

Figura 24 Topografía del escenario 2



6.7. Desarrollo escenario 2

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario
2. Configurar el protocolo de enrutamiento OSPFv2
3. Visualizar tablas de enrutamiento y routers conectados por OSPFv2
4. Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
5. Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada Router.
6. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
7. En el Switch 3 deshabilitar DNS lookup
8. Asignar direcciones IP a los Switches acorde a los lineamientos.
9. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

10. Implement DHCP and NAT for IPv4
11. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
12. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.
13. Configurar NAT en R2 para permitir que los hosts puedan salir a internet
14. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
15. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
16. Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

7 CONCLUSIONES

La versión 2 del Router Rip incluye la máscara de subred en la tabla de enrutamiento, soportando VLSM en el diseño de la topología.

En el escenario 1 Al verificar los equipos se puede detallar un direccionamiento entre los R1, R2 y R#, mediante la configuración previa utilizando un direccionamiento Route Rip.

en el desarrollo de los diferentes escenarios se ha aplicado el conocimiento adquirido en el curso de profundización del CCNA

el protocolo Routing Information Protocol (RIP) es un protocolo muy común en la configuración de redes,
en un protocolo vector distancia, que calcula cual sería la mejor ruta para el direccionamiento de paquetes IP, utiliza como métrica el número de saltos Hop Count, hasta 15 saltos, de ahí en adelante la descarta como inalcanzable.

8 REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

Guía De Actividades Prueba De Habilidades Practicas Https://Static-Course-Assets.S3.Amazonaws.Com/Rse503/Es/Index.Html#3.2 Laboratorios Smarlab

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf